PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G05B 9/03

A1

(11) Internationale Veröffentlichungsnummer: **WO 98/53374**

(43) Internationales Veröffentlichungsdatum: 26. November 1998 (26.11.98)

(21) Internationales Aktenzeichen: PCT/EP98/01108

(22) Internationales Anmeldedatum: 27. Februar 1998 (27.02.98)

(30) Prioritätsdaten:
197 20 618.2 16. Mai 1997 (16.05.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: ITT MANUFACTURING ENTERPRISES, INC. [US/US]; Suite 1217, 1105 North Market Street, Wilmington, DE 19801 (US).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: GIERS, Bernhard [DE/DE]; Kaiser–Sigmund–Strasse 60, D–60320 Frankfurt am Main (DE).

(74) Anwälte: BLUM, K.–D. usw.; ITT Automotive Europe GmbH, Guerickestrasse 7, D–60488 Frankfurt am Main (DE).

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

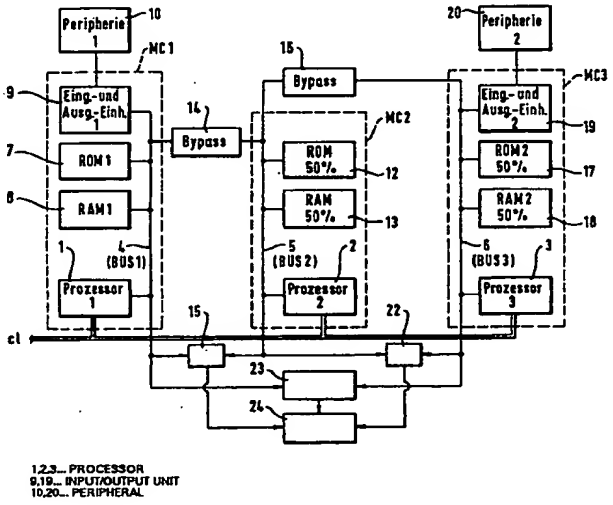
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: MICROPROCESSOR SYSTEM FOR AUTOMOBILE CONTROL SYSTEMS

(54) Bezeichnung: MIKROPROZESSORSYSTEM FÜR KFZ–REGELUNGSSYSTEME

(57) Abstract

The invention relates to a microprocessor system for safety–critical control systems, which is provided with three central processing units (1, 2, 3) jointly arranged on a chip and which process the same program. The system also comprises read–only memories (7, 12, 17) and read–write–memories (8, 13, 18), input and output units (9, 19) and comparators (15, 22, 23), which check the output signals of the central processing units (1, 2, 3) to see whether they match. The central processing units (1, 2, 3) are interconnected by means of bus systems (4, 5, 6) and bypasses (14, 16), which enable the central processing units (1, 2, 3) to read and process the existing data and commands according to the same program. The storage capacity of the read–only memories and the read–write memories is at least double that of a memory required for a non–redundant system. Storage space is, for instance, divided among the following system in a ratio of 100:50:50. Redundant peripheral components (10, 20) provide the central processing units (1, 2, 3) with two complete control signal circuits which are interconnected so that a defective central processing unit (1, 2, 3) can be identified in case of failure by a majority decision and switching to an emergency operational function can take place.



(57) Zusammenfassung

Ein Mikroprozessorsystem für sicherheitskritische Regelungen ist mit drei, gemeinsam auf einem Chip angeordneten Zentraleinheiten (1, 2, 3) ausgerüstet, die das gleiche Programm abarbeiten. Außerdem sind Festwertspeicher (7, 12, 17) und Schreib–Lese–Speicher (8, 13, 18), Eingabe– und Ausgabeeinheiten (9, 19) und Vergleicher (15, 22, 23) vorhanden, die die Ausgangssignale der Zentraleinheiten (1, 2, 3) auf Übereinstimmung überprüfen. Die Zentraleinheiten (1, 2, 3) sind über Bus–Systeme (4, 5, 6) und über Bypässe (14, 16) untereinander verbunden, die den Zentraleinheiten (1, 2, 3) ein gemeinsames Lesen und Abarbeiten der anstehenden Daten und Befehle nach dem gleichen Programm ermöglichen. Die Speicherkapazität der Festwert– und der Schreib–Lese–Speicher beträgt insgesamt mindestens 200 % im Vergleich zu dem für ein nicht redundantes System benötigten Speicher. Die Speicherplätze sind auf die drei Systeme z.B. im Verhältnis 100:50:50 verteilt. Die Zentraleinheiten (1, 2, 3) sind durch redundante Peripherie–Komponenten (10, 20) zu zwei vollständigen Regelunssignalkreisen erweitert und derart zusammengeschaltet, daß bei einem Ausfall durch Majoritätsentscheid die fehlerhafte Zentraleinheit (1, 2, 3) identifiziert und ein Übergang zu einer Notlauffunktion erfolgen kann.

Mikroprozessorsystem für KFZ-Regelungssysteme

Die Erfindung bezieht sich auf ein Mikroprozessorsystem der im Oberbegriff des Hauptanspruchs beschriebenen Art. Es handelt sich also um ein System für sicherheitskritische Regelungen, mit redundanter Datenverarbeitung, mit mehreren Zentraleinheiten, welche über separate Bus-Systeme mit Festwertspeichern und Schreib-Lesespeichern, mit Eingabe- und Ausgabeeinheiten und mit Vergleichern, die die die Ergebnisse und/oder Zwischenergebnisse der Datenverarbeitung auf Übereinstimmung überprüfen, zu mehreren Datenverarbeitungssystemen verbunden sind, wobei die Zentraleinheiten über die Bus-Systeme miteinander kommunizieren und das gleiche Programm abarbeiten und wobei die Bus-Systeme untereinander durch Bypässe verbunden sind, die den Zentraleinheiten ein gemeinsames Lesen und Abarbeiten der anstehenden Daten und Befehle ermöglichen.

Zu den sicherheitskritischen Regelungen dieser Art zählen u.a. die in die Bremsenfunktion eines Kraftfahrzeugs eingreifenden Regelungssysteme, die in großer Anzahl und großer Vielfalt auf dem Markt sind. Beispiele hierfür sind die Antiblockiersysteme (ABS), Antriebsschlupfregelungssysteme (ASR), Fahrstabilitätsregelungen (FDR,ASMS), Fahrwerksregelungssysteme etc. Ein Ausfall eines solchen Regelungssystems führt zur Gefährdung der Fahrstabilität des Fahrzeugs. Daher wird die Funktionsfähigkeit der Systeme ständig überwacht, um beim Auftreten eines Fehlers die Regelung abschalten oder in einen für die Sicherheit weniger gefährlichen Zustand um-

schalten zu können. Noch kritischer sind Bremssysteme bzw. Kraftfahrzeug-Regelungssysteme, bei denen bei Ausfall der Elektronik keine Umschaltung auf ein mechanisches oder hydraulisches System möglich ist. Hierzu zählen Bremssystemkonzepte, wie "Brake-by-wire", die voraussichtlich in der Zukunft noch an Bedeutung gewinnen werden; die Bremsenfunktion ist bei solchen Systemen auf eine intakte Elektronik angewiesen.

Ein Beispiel für ein Microprozessorsystem zur Steuerung und Überwachung einer blockiergeschützten Fahrzeugbremsanlage ist aus der DE 32 34 637 C2 bekannt. Nach dieser Schrift werden die Eingangsdaten zwei identisch programmierten Microcomputern parallel zugeführt und dort synchron verarbeitet. Die Ausgangssignale und Zwischensignale der beiden Microcomputern werden auf Übereinstimmung geprüft. Wenn die Signale voneinander abweichen, wird die Regelung abgeschaltet.

Nach einem anderen bekannten System, nach dem die in der DE 41 37 124 A1 beschriebene Schaltung aufgebaut ist, werden die Eingangsdaten ebenfalls zwei Microcomputern parallel zugeführt, von denen jedoch nur einer die vollständige, aufwendige Signalverarbeitung ausführt. Der zweite Microcomputer dient vornehmlich zur Überwachung, weshalb die Eingangssignale nach Aufbereitung, Bildung von zeitlichen Ableitungen etc. mit Hilfe vereinfachter Regelalgorithmen und vereinfachter Regelpilosophie weiterverarbeitet werden können. Die vereinfachte Datenverarbeitung reicht zur Erzeugung von Signalen aus, die durch Vergleich mit den in dem aufwendige-

ren Microcomputer verarbeiteten Signalen Rückschlüsse auf den ordnungsgemäßen Betrieb des Systems zulassen.

Aus der DE 43 41 082 A1 ist ein Mikroprozessorsystem bekannt, das insbesondere für das Regelsystem einer blockiergeschützten Bremsanlage vorgesehen ist. Dieses bekannte System, das auf einem einzigen Chip untergebracht werden kann, enthält zwei Zentraleinheiten, in denen die Eingangsdaten parallel verarbeitet werden. Die Festwert- und die Schreib-Lese-Speicher, die an die beiden Zentraleinheiten angeschlossen sind, enthalten zusätzliche Speicherplätze für Prüfinformationen und umfassen jeweils einen Generator zur Erzeugung von Prüfinformationen. Die Ausgangssignale eines der beiden Zentraleinheiten werden zur Erzeugung der Steuersignale weiterverarbeitet, während die andere als passive Zentraleinheit lediglich zur Überwachung der aktiven Zentraleinheit dient.

Schließlich ist aus der DE 195 29 434 A1 bereits ein System der eingangs genannten Art bekannt, bei dem zwei synchron betriebene Zentraleinheiten auf einem oder auf mehreren Chips vorgesehen sind, die die gleichen Eingangsinformationen erhalten und das gleiche Programm abarbeiten. Die beiden Zentraleinheiten sind dabei über separate Bus-Systeme an die Festwert- und an die Schreib-Lese-Speicher sowie an Eingabe- und Ausgabeeinheiten angeschlossen. Die Bus-Systeme sind untereinander durch Treiberstufen bzw. Bypässe verbunden sind, die den beiden Zentraleinheiten ein gemeinsames Lesen und Abarbeiten der zur Verfügung stehenden Daten und Befehle ermöglichen. Das System ermöglicht eine Einsparung von Speicherplatz. Nur eine der beiden Zentraleinheiten ist (direkt) mit einem vollwertigen Festwert- und einem Schreib-Lese-Speicher verbunden, während die Speicherkapazität des zweiten Prozessors auf Speicherplätze für Prüfdaten (Paritätsüberwachung) in Verbindung mit einem Prüfdatengenerator be

schränkt ist. Zugriff zu allen Daten besteht über die Bypäse. Dadurch sind beide Zentraleinheiten in der Lage, jeweils das vollständige Programm abzuarbeiten.

Alle vorgenannten Systeme beruhen grundsätzlich auf dem Vergleich redundant verarbeiteter Daten und der Erzeugung eines Fehlersignals, wenn Abweichungen auftreten. Beim Auftreten eines Fehlers oder Ausfall eines Systems kann dann die Regelung abgeschaltet werden. In keinem Fall ist eine Notlauffunktion, nämlich einer Fortsetzung der Regelung nach dem Auftreten des Fehlers, möglich. Eine solche Notlauffunktion wäre grundsätzlich nur durch Verdoppelung der Systeme in Verbindung mit einem Identifizieren und Abschalten der Fehlerquelle denkbar.

Der vorliegenden Erfindung liegt nun die Aufgabe zugrunde, ein Mikroprozessorsystem der eingangs genannten Art mit höchstens geringem Mehraufwand derart auszugestalten, daß beim Auftreten eines Fehlers eine Notlauffunktion möglich wird.

Es hat sich herausgestellt, daß diese Aufgabe durch das im Anspruch 1 beschriebene Mikroprozessorsystem gelöst werden kann. Die Besonderheit dieses Systems besteht darin, daß mindestens drei Zentraleinheiten mit insgesamt mindestens doppelter Speicherkapazität im Vergleich zu der für ein nicht redundantes System benötigten Speicherkapazität vorhanden sind, daß die Zentraleinheiten durch redundante Periphere-Einheiten zu mindestens zwei vollständigen Regelungssignalkreisen erweitert und derart zusammengeschaltet sind, daß bei Ausfall einer Zentraleinheit und/oder zugehöriger Komponenten bzw. beim Auftreten eines Fehlers in einem der Datenverarbeitungssysteme durch Majoritätsentscheidung in einer Identifizierungsstufe die fehlerbehaftete Zentraleinheit identifizierbar ist, ein Übergang in eine Notlauf-

funktion erfolgt, in der mindestens ein Regelungssignalkreis mit voller Speicherkapazität zur Verfügung steht und eine Ausgabe von Ausgangssignalen oder Steuersignalen in Abhängigkeit von der fehlerbehafteten Zentraleinheit verhindert wird.

Erfindungsgemäß wird zugunsten eines besonders einfachen Regleraufbaus in bestimmten, seltenen Fällen auf eine Redundanz, d.h. auf eine Aufrechterhaltung der redundanten Datenverarbeitung verzichtet, weil das Auftreten eines weiteren Fehlers während einer kurzen Notlaufphase denkbar unwahrscheinlich ist und weil eine Abschaltung der Regelung nicht infrage kommt oder ein höheres Sicherheitsrisiko zur Folge hätte. Statt dessen werden beim Auftreten von Fehlern nach dem Identifizieren der Fehlerquelle bzw. der intakten Systeme die Auswirkungen von Fehlern unterbunden und die Steuerung und/oder Regelung auf Basis der fehlerfreien Systeme und Signale fortgesetzt.

Nach einem vorteilhaften Ausführungsbeispiel der Erfindung sind drei Zentraleinheiten mit je einem Bus-System vorgesehen und die Speicherplätze in den drei Zentraleinheiten derart verteilt angeordnet, daß bei Ausfall einer Zentraleinheit den beiden übrigen insgesamt mindestens die volle Festwert- und Schreib-Lese-Speicherkapazität zur Verfügung steht, wobei über die Bypässe alle Zentraleinheiten mit den Speicherplätzen in Schreib- und Leserichtung und mit allen Eingabe- und Ausgabeeinheiten verbunden sind.

Als besonders zweckmäßig hat es sich dabei erwiesen, eine Zentraleinheit mit der vollen (100%), die beiden anderen mit jeweils mindestens 50% der für ein nicht redundantes System benötigten Festwert- und Schreib-Lese-Speicherkapazität auszurüsten.

Die Erfindung geht gewissermaßen von dem vorgenannten, aus der DE 195 29 434 A1 bekannten System aus, das im Prinzip aus einem vollständigen und einem unvollständigen Datenverarbeitungssystem besteht, und erweitert dieses System durch ein zusätzliches, vollständiges Datenverarbeitungssystem mit den zugehörigen Peripherie-Einheiten. Auf diese Weise entstehen zwei vollständige Regelungssignalkreise oder Regelungssignalverarbeitungssysteme, die zu einem notlauffähigen Gesamtsystem zusammengeschaltet sind, das auch bei Ausfall eines Prozessors und Identifizieren der Fehlerquelle eine Aufrechterhaltung der Regelung erlaubt. Durch die erfindungsgemäße Zusammenschaltung der einzelnen Systeme oder Komponenten wird bei Ausfall eines Prozessors eine Fortsetzung der Steuerung und Regelung durch Einsatz der intakten Kreise möglich.

Der Gesamtaufwand an Speicherplätzen, der wesentlich den Preis des Mikroprozessorsystems bestimmt, wird im Vergleich zu einer Verarbeitung in einem nicht redundanten System lediglich verdoppelt, wobei die Aufteilung und Zuordnung der Speicherplätze zu den einzelnen Prozessoren in weiten Grenzen variabel ist; es muß sichergestellt sein, daß jeder einzelne Prozessor bzw. jede einzelne Prozessoreinheit das volle Programm abarbeiten kann.

Die erfindungsgemäße Ausgestaltung des Mikroprozessorsystems ermöglicht die Unterbringung aller oder der wesentlichen Komponenten, insbesondere sämtlicher Zentraleinheiten, Speicher, der Vergleicher und der Bypässe sowie ggf. auch der Eingabe- und Ausgabeeinheiten, auf einem einzigen Chip.

Die drei Zentraleinheiten bilden zusammen mit den Speichern, mit den Eingabe- und Ausgabeeinheiten und mit den Peripherie-Einheiten, einschließlich der Spannungsversorgung etc., insgesamt zwei vollständige und ein unvollständiges

Datenverarbeitungssystem; die für einen vollständigen Programmablauf benötigten Speicherplätze sind auf die Datenverarbeitungssysteme aufgeteilt. Diese Datenverarbeitungssysteme umfassen vorteilhafterweise jeweils eine Zentraleinheit, ein Bus-System sowie Festwert- und Schreib-Lese-Speicher, wobei die Speicherplätze derart auf die einzelnen Datenverarbeitungssysteme verteilt sind, daß beim Auftreten eines Fehlers und Übergang zur Notlauffunktion die intakten Systeme ausreichend Speicherplätze für die komplette Datenverarbeitung enthalten und das komplette Programm abarbeiten.

Ein weiteres Ausführungsbeispiel nach der Erfindung besteht darin, daß dieses für mehrere oder eine Kombination von Kraftfahrzeug-Regelungssystemen, wie Brake-by-wire, ABS, ASR, ASMS etc., ausgelegt ist, wobei die Notlauffunktion entweder die Aufrechterhaltung des Betriebs aller Regelungssysteme erfaßt oder nur auf die Aufrechterhaltung ausgewählter Regelungsfunktionen, zum Beispiel besonders sicherheitskritischer Funktionen, beschränkt ist.

In den Unteransprüchen sind noch weitere vorteilhafte Ausführungsbeispiele beschrieben.

Aus der beigefügten Abbildung, welche in schematisch vereinfachter Darstellung die wesentlichen Komponenten eines Mikroprozessorsystems nach der Erfindung wiedergibt, und aus der nachfolgenden Beschreibung gehen weitere Einzelheiten der Erfindung hervor. Diese Abbildung dient zur Erläuterung des prinzipiellen Aufbaus und der Wirkungsweise eines Ausführungsbeispiels der Erfindung.

Die Abbildung bezieht sich auf ein Ein-Chip-Mikrocomputersystem, das drei synchron betriebene Prozessoren oder Zentraleinheiten 1,2,3, die auch als Rechner- oder, wegen ihrer

Funktion, als Prozessorkerne bezeichnet werden. Jedem Prozessor ist ein Bus-System 4,5,6 zugeordnet. Die Zentraleinheiten 1,2,3 sind an eine synchrone Taktversorgung cl (common clock), die redundant ausgelegt ist, angeschlossen.

Die Zentraleinheit 1 bzw. der Prozessorkern 1 ist durch einen Festwertspeicher 7 (ROM 1), durch einen Schreib-Lese-Speicher 8 (RAM 1), durch eine Eingabe- und Ausgabeeinheit 9 zu einem vollständigen Datenverarbeitungssystem oder Mikrocomputer MC1 ergänzt. Die notwendigen Peripheriekomponenten (Peripherie 1) sind durch einen externen Block 10 symbolisiert. Zu den Peripheriekomponenten zählen die Spannungsversorgung, die Zuführung der Eingangssignale (z.B. der Sensorsignale bei einem KFZ-Regelungssystem) und die Aktuator- oder Ventilansteuerung etc. mit Hilfe der Ausgangsdaten oder -signale der Datenverarbeitungssysteme.

Ein zweites, unvollständiges Datenverarbeitungssystem oder ein Mikrocomputer MC2, in dem die Zentraleinheit 2 untergebracht ist, enthält im wiedergegebenen Ausführungsbeispiel lediglich Speicherplätze für 50% der für ein nicht redudantes System benötigten Daten. Symbolisch dargestellt sind im Inneren des Mikrocomputers MC2 Festwertspeicherplätze 12 und Speicherplätze 13 für die Daten im Schreib-Lese-Bereich.

Über einen Bypass 14 sind BUS 1 (Bus-System 4) und BUS 2 (Bus-System 5) miteinander verbunden. Der Bypass 14 ermöglicht der Zentraleinheit 1 ein Lesen der in den Speicherplätzen 12, 13 gespeicherten Daten und gestattet einen Datenfluß von den Speichern 7,8 und dem Prozessorkern 1 des Mikrocomputers MC1 zu dem Mikrocomputer MC2, insbesondere zu der Zentraleinheit 2. Auf diese Weise ist ein redundantes Abarbeiten des vollständigen Datenverarbeitungs-Programms durch beide Zentraleinheiten 1,2 gewährleistet. Noch weitere Einzelheiten zu dem Aufbau und der Funktionsweise solcher

Mikroprozessorsysteme sind der vorgenannten DE 195 29 434 A1 zu entnehmen.

Die Datenverarbeitungs-Ergebnisse beider Systeme MC1, MC2 bzw. Prozessoren 1,2 werden, wie ebenfalls in der vorgenannten Schrift erläutert ist, mit Hilfe eines Vergleichers 15 auf Übereinstimmung überwacht; es ist ein unmittelbarer Vergleich der Ausgangssignale beider Prozessoren mit Hilfe eines Hardware-Vergleichers 15 vorgesehen.

Ein wesentliches Merkmal des Mikroprozessorsystems nach der Erfindung und des in der Abbildung dargestellten Ausführungsbeispiels besteht nun darin, daß das eben beschriebene, aus der DE 195 29 434 A1 bekannte System durch ein weiteres Datenverarbeitungssystem, nämlich durch einen Mikrocomputer MC3, der ebenfalls mit dem unvollständigen Mikrocomputer MC2 und auch mit dem Mikrocomputer MC1 zusammenwirkt, erweitert ist. Ein Teil der Funktionen dieses zusätzlichen Mikrocomputersystems (MC3), nämlich das Speichern eines Teils der Daten, z.B. von 50% der Festwert- und der Schreib-Lese-Daten, wird allerdings von dem zweiten Mikrocomputersystem MC2 und ggf. auch von dem ersten System MC1 wahrgenommen, weil das Gesamtsystem für die Gewährleistung der Redundanzfunktion insgesamt nur die doppelte Speicherkapazität im Vergleich zu einem nicht redundanten, das gleiche Programm abarbeitenden System benötigt. Die Speicherkapazität muß dabei auf die drei Datenverarbeitungssysteme MC1, MC2, MC3 derart verteilt werden, daß bei Ausfall eines Systems die verbleibenden Systeme einen ausreichenden Speicherplatz, nämlich mindestens 100%, bieten. In einen bevorzugten Ausführungsbeispiel sind das Mikroprozessorsystem MC1 mit 100%, die beiden Mikrocomputersysteme MC2 und MC3 mit jeweils 50% der für ein nicht redundantes System benötigten Speicherplätze ausgerüstet.

Das dritte Mikrocomputersystem MC3 ist mit dem (unvollständigen) Mikrocomputer MC2 ebenfalls durch einen Bypass 16 verbunden. Dieser Bypass hat die gleiche Funktion wie der bereits eingehend beschriebene Bypass 14 und ermöglicht daher auch den Zentraleinheiten 2 und 3 die redundante Verarbeitung aller Eingangsdaten.

Das Mikroprozessorsystem MC3 enthält einen Festwertspeicher 17 (ROM 2), einen Schreib-Lese-Speicher 18 (RAM 2), eine Eingabe- und Ausgabeeinheit 19 und Peripherie-Komponenten 20 (Peripherie 2). MC3 ist im dargestellten Ausführungsbeispiel ein vollständige Mikrocomputer, für den allerdings, wie zuvor erläutert, eine reduzierte Speicherkapazität genügt; die Kapazität der Speicher in MC2 Und MC3 beträgt zusammen (mindestens) 100%.

Über die Bypässe 14,16 ist ein Datenfluß in beiden Richtungen vom BUS 1 (Bus-System 4) zum BUS 3 (Bus-System 6) gegeben. Zur weiteren Erhöhung der Ausfallsicherheit könnte es eventuell sinnvoll sein, über einen zusätzlichen Bypass, der nicht dargestellt ist, eine direkte Verbindung zwischen diesen beiden Bus-Systemen 4,6 (BUS 1 und BUS 3) herzustellen.

Der Mikrocomputer MC3 besitzt hier den gleichen Aufbau und die gleichen Komponenten wie der Mikrocomputer MC1. Folglich sind bei dem erfindungsgemäßen Mikroprozessorsystem auch die Eingabe- und Ausgabeeinheiten 9,19 und die Peripherie-Komponenten 10, 20, zu denen die Spannungsversorgung, der Sensorsignaleingang und die Aktuatoransteuerung zählen, zweimal vorhanden.

Die Ausgangssignale oder Datenverarbeitungsergebnisse des dritten Mikrocomputers MC3 werden mit Hilfe eines Vergleichers 22 auf Übereinstimmung mit den Ergebnissen oder Ausgangssignalen des Mikrocomputers MC2 bzw. der Zentraleinheit

2 sowie in gleicher Weise mit Hilfe des Vergleichers 23 auf Übereinstimmung mit den Ergebnissen des MC1 bzw. der Zentraleinheit 1 überprüft. Dadurch ist nicht nur eine Fehlererkennung, sondern auch eine Identifizierung des Systems, in dem der Fehler liegt, möglich. In einer Identifizierungs-Stufe 24, die vorzugsweise redundant ausgeführt ist und der die Ausgangssignale der Vergleicher 15,22,23 zugeleitet werden, wird durch eine Majoritätsentscheidung die Fehlerquelle erkannt und daraufhin das System auf eine Notlauffunktion umgeschaltet. Dies bedeutet, daß die Ausgabe von Steuersignalen in Abhängigkeit von den fehlerhaften Datenverarbeitungsergebnissen verhindert und statt dessen auf das intakte System umgeschaltet wird.

Das erfindungsgemäße System läßt sich mit vergleichsweise geringem Herstellungsaufwand realisieren. Im Prinzip genügt - im Vergleich zu dem bekannten System, das keinen Notlauf zuläßt - das Hinzufügen eines Prozessorkerns und die Erhöhung der Speicherkapazität auf das Doppelte. Eine klassische Lösung mit Notlauffunktion würde mindestens den dreifachen Speicheraufwand erfordern.

Wird die Speicherkapazität um einige Speicherplätze im Vergleich zu dem Minimalwert von 200% erhöht, z.B. um Speicherplätze für je ein Paritätsbit, ist eine Fehlerlokalisierung im Speicherbereich auch über Hardware-Majoritätsentscheid möglich. Wird die Minimalauslegung der Speicherkapazität von 200% gewählt,läßt sicht eine Fehlerlokalisierung z.B. durch Quersummenbildung über Speicherblöcke oder durch andere software-technische Maßnahemen realisieren.

Die mit Hilfe der erfindungsgemäßen Auslegung erreichte Reduzierung der Speicherkapazität im Vergleich zu den bekannten Systemen ist ein entscheidender Vorteil, weil die Kosten

des Gesamtsystems maßgeblich von der Größe der Arbeitsspeicher (Festwert- und Schreib-Lese-Speicher) bestimmt werden.

Der Aufwand für die Vergleicher 15, 22, 23, die eine Identitätsüberwachung durchführen, ist minimal. Der Austausch von Signalen zwischen den einzelnen Mikrocomputern über die Bypässe erfordert keinen nennenswerten Aufwand. Programmtechnisch wird eine Software für ein scheinbares Einprozessorsystem realisiert; es werden keine Softwarestrukturen benötigt, die einen Austausch von Signalen zwischen den Mikrocomputern realisieren oder Signale auf Gleichheit oder Ähnlichkeit überprüfen.

Grundsätzlich ist es auch möglich, beim Auftreten eines internen Rechnerfehlers die Übernahme der Eingangsinformation und der Signalausgabe durch den fehlerfreien Kreis durchzuführen bzw. dem fehlerfreien Kreis zu übertragen. Dies führt zu weiteren Vereinfachungen und Systemfunktionen.

Patentansprüche

1. Mikroprozessorsystem für KFZ-Regelungssysteme, insbesondere für sicherheitskritische Regelungen, mit redundanter Datenverarbeitung , mit mehreren Zentraleinheiten (CPU), die über separate Bus-Systeme mit Festwertspeichern und Schreib-Lesespeichern, mit Eingabe- und Ausgabeeinheiten und mit Vergleichern, die die die Ergebnisse und/oder Zwischenergebnisse der Datenverarbeitung auf Übereinstimmung überprüfen, zu mehreren Datenverarbeitungssystemen verbunden sind, wobei die Zentraleinheiten über die Bus-Systeme miteinander kommunizieren und das gleiche Programm abarbeiten und wobei die Bus-Systeme untereinander durch Bypässe verbunden sind, die den Zentraleinheiten ein gemeinsames Lesen und Abarbeiten der anstehenden Daten und Befehle ermöglichen, dadurch **gekennzeichnet**, daß mindestens drei Zentraleinheiten (1,2,3) mit insgesamt mindestens doppelter Speicherkapazität im Vergleich zu der für ein nicht redundantes System benötigten Speicherkapazität vorhanden sind, daß die Zentraleinheiten (1,2,3) durch redundante Periphere-Einheiten (10,20) zu mindestens zwei vollständigen Regelungssignalkreisen erweitert und derart zusammengeschaltet sind, daß bei Ausfall einer Zentraleinheit (1,2,3) und/oder einer zugehörigen Komponente bzw. beim Auftreten eines Fehlers in einem der Datenverarbeitungssysteme durch Majoritätsentscheidung in einer Identifizierungsstufe (24) die fehlerbehaftete Zentraleinheit (1,2,3) identifizierbar ist, ein Übergang in eine Notlauffunktion erfolgt, in der mindestens ein Regelungssignalkreis mit voller Speicherkapazität zur Verfügung steht und eine Ausgabe von Ausgangssignalen oder Steuersignalen in Abhängigkeit von der fehlerbehafteten Zentraleinheit verhindert wird.

2. Mikroprozessorsystem nach Anspruch 1 , dadurch **gekennzeichnet**, daß drei Zentraleinheiten (1,2,3) mit je einem Bus-System (4,5,6) vorgesehen sind und daß die Speicherplätze in den drei Zentraleinheiten (1,2,3) derart verteilt angeordnet sind, daß beim Auftreten eines Fehlers in einem der Datenverarbeitungssysteme (MC1,MC2,MC3) oder bei Ausfall einer Zentraleinheit den beiden übrigen insgesamt mindestens die volle Festwert- und Schreib-Lese-Speicherkapazität (7,12,17; 8,13,18) zur Verfügung steht, wobei über die Bypässe (14,16) alle Zentraleinheiten (1,2,3) mit den Speicherplätzen in Schreib- und Leserichtung und mit allen Eingabe- und Ausgabeeinheiten (9,10) verbunden sind.

3. Mikroprozessorsystem nach Anspruch 2, dadurch **gekennzeichnet**, daß eine Zentraleinheit (1,2,3) mit der vollen, die beiden anderen mit jeweils mindestens 50% der für ein nicht redundantes System benötigten Festwert- und Schreib-Lese-Speicherkapazität ausgerüstet sind.

4. Mikroprozessorsystem nach Anspruch 2 oder 3, dadurch **gekennzeichnet**, daß die drei Zentraleinheiten (1,2,3) zusammen mit den Speichern (7,8,12,13,17,18), mit den Eingabe- und Ausgabeeinheiten (9,10) und mit den Peripherie-Komponenten (10,20) insgesamt zwei vollständige und ein unvollständiges Datenverarbeitungssystem bilden.

5. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß den Vergleichern (15,22,23) jeweils die Datenverarbeitungsergebnisse bzw. Ausgangssignale von zwei Zentraleinheiten (1,2,3) zuführbar sind.

6. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß zumindest die Zentraleinheiten (1,2,3) mit den Bus-Systemen (4,5,6), die Speicher (7,8,12,13,17,18), die Bypässe (14,16), die Eingabe- und Ausgabeeinheiten (9,19), Vergleicher (15,22,23) und Identifizierungsstufen (24) auf einem gemeinsamen Chip angeordnet sind.

7. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, daß dieses für mehrere oder eine Kombination von Kraftfahrzeug-Regelungssystemen, wie Brake-by-wire, ABS, ASR, ASMS etc., ausgelegt ist und daß die Notlauffunktion die Aufrechterhaltung des Betriebs aller Regelungssysteme erfaßt.

8. Mikroprozessorsystem nach einem oder mehreren der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, daß dieses für mehrere oder eine Kombination von Kraftfahrzeug-Regelungssystemen ausgelegt ist und daß die Notlauffunktion auf die Aufrechterhaltung des Betriebs ausgewählter Regelungsfunktionen, zum Beispiel besonders sicherheitskritischer Funktionen, beschränkt ist.

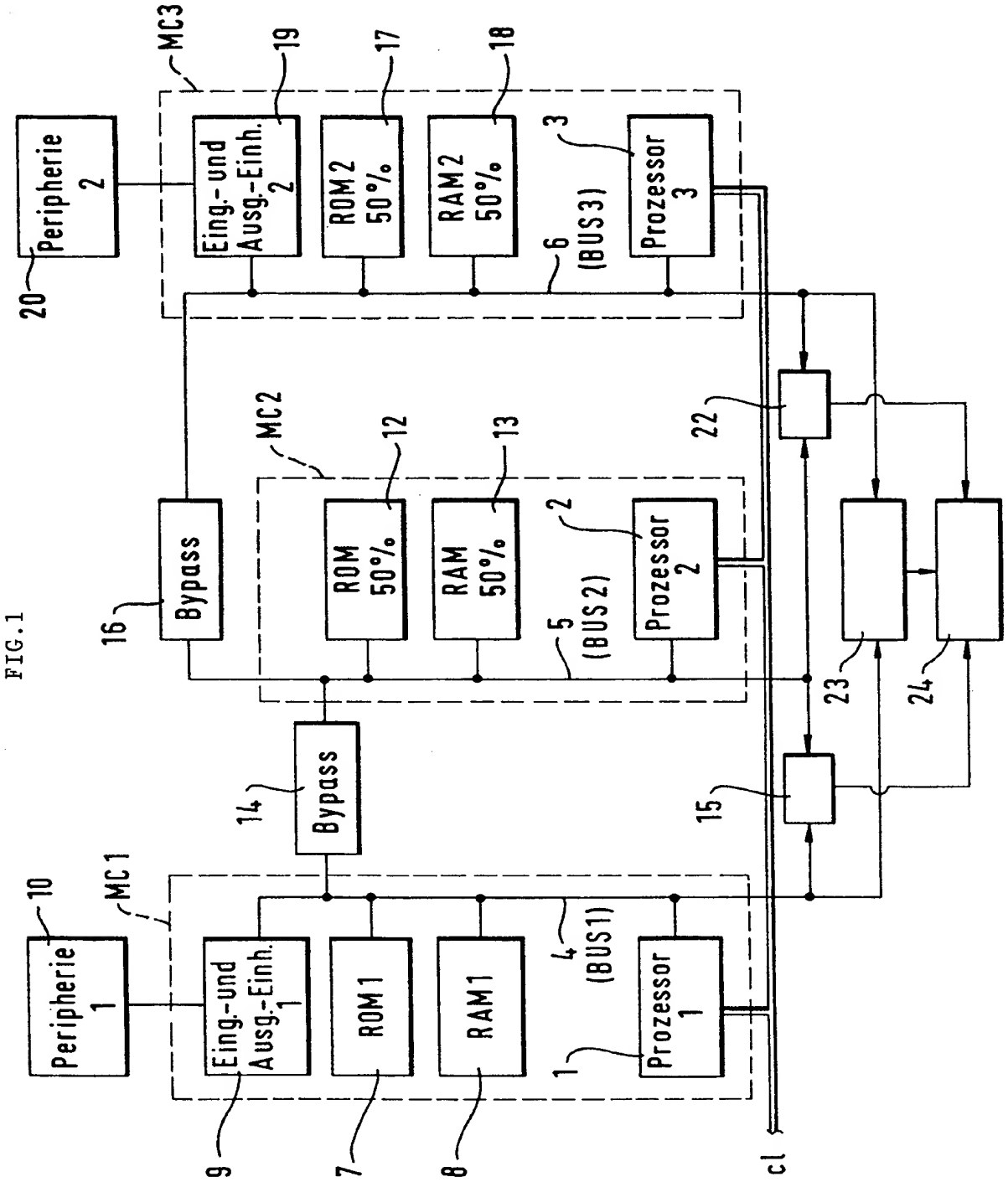

MC3
MC2
MC1
Peripherie 2
Eing.-und Ausg.-Einh. 2
ROM2 50%
RAM2 50%
Prozessor 3
(BUS3)
Bypass
ROM 50%
RAM 50%
Prozessor 2
(BUS2)
Bypass
Peripherie 1
Eing.-und Ausg.-Einh. 1
ROM 1
RAM1
Prozessor 1
(BUS1)
cl
20
19
17
18
3
6
16
12
13
2
5
22
14
15
23
24
10
9
7
8
4
1

FIG.1

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/EP 98/01108

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G05B9/03

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G05B

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SMITH S E: "TRIPLE REDUNDANT FAULT TOLERANCE: A HARDWARE-IMPLEMENTED APPROACH" ISA TRANSACTIONS, vol. 30, no. 4, 1 January 1991, pages 87-95, XP000275596 see the whole document ---	1
A	US 4 672 530 A (SCHUSS JACK A) 9 June 1987 see the whole document ---	1
A	EP 0 399 308 A (AEG WESTINGHOUSE TRANSPORT) 28 November 1990 see the whole document ---	1
A	US 5 583 769 A (SAITOH HIROO) 10 December 1996 see column 4, line 7 - column 7, line 10 ---	1

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theInternational search	Date of mailing of the international search report
23 June 1998	30/06/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kelperis, K

3

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/EP 98/01108

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 32 25 455 A (SIEMENS AG) 19 January 1984 see the whole document	1
A	DE 32 34 637 A (TEVES GMBH ALFRED) 22 March 1984 cited in the application see the whole document	1
A	DE 43 41 082 A (TEVES GMBH ALFRED) 8 June 1995 cited in the application see the whole document	1
A	DE 41 37 124 A (TEVES GMBH ALFRED) 13 May 1993 cited in the application see the whole document	1
A	EP 0 346 804 A (ALSTHOM) 20 December 1989 see the whole document	1
A	DE 195 29 434 A (TEVES GMBH ALFRED) 13 February 1997 cited in the application see the whole document	1
A	GUDEA D D ET AL: "FAULT TOLERANT POWER CONTROLLER" PROCEEDINGS OF THE INTERSOCIETY ENERGY CONVERSION ENGINEERING CONFERENCE. (IECEC), WASHINGTON, AUG. 6 - 11, 1989, vol. VOL. 1, no. CONF. 24, 6 August 1989, JACKSON W D;HULL D A, pages 231-237, XP000078771 see the whole document	1

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/EP 98/01108

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4672530 A	09-06-1987	IN 163485 A	01-10-1988
EP 0399308 A	28-11-1990	US 5086499 A	04-02-1992
		CA 2017227 A,C	23-11-1990
		JP 3012772 A	21-01-1991
US 5583769 A	10-12-1996	JP 4133601 A	07-05-1992
		KR 9505875 B	02-06-1995
DE 3225455 A	19-01-1984	NONE	
DE 3234637 A	22-03-1984	FR 2533183 A	23-03-1984
		GB 2127507 A,B	11-04-1984
		JP 59130768 A	27-07-1984
		US 4546437 A	08-10-1985
DE 4341082 A	08-06-1995	WO 9515518 A	08-06-1995
		EP 0731937 A	18-09-1996
		JP 9509269 T	16-09-1997
DE 4137124 A	13-05-1993	CZ 9203808 A	16-03-1994
		DE 59202984 D	24-08-1995
		WO 9309986 A	27-05-1993
		EP 0611352 A	24-08-1994
		HU 69338 A	28-09-1995
		JP 7504864 T	01-06-1995
		PL 168757 B	30-04-1996
		SK 380892 A	07-06-1995
		US 5458404 A	17-10-1995
EP 0346804 A	20-12-1989	FR 2632748 A	15-12-1989
		CN 1041465 A,B	18-04-1990
		EG 18885 A	30-11-1994
		JP 2039245 A	08-02-1990
		MX 172185 B	07-12-1993
DE 19529434 A	13-02-1997	WO 9706487 A	20-02-1997
		EP 0843853 A	27-05-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/01108

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G05B9/03

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	SMITH S E: "TRIPLE REDUNDANT FAULT TOLERANCE: A HARDWARE-IMPLEMENTED APPROACH" ISA TRANSACTIONS, Bd. 30, Nr. 4, 1.Januar 1991, Seiten 87-95, XP000275596 siehe das ganze Dokument ---	1
A	US 4 672 530 A (SCHUSS JACK A) 9.Juni 1987 siehe das ganze Dokument ---	1
A	EP 0 399 308 A (AEG WESTINGHOUSE TRANSPORT) 28.November 1990 siehe das ganze Dokument ---	1
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23.Juni 1998	30/06/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kelperis, K

3

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/01108

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 583 769 A (SAITOH HIROO) 10.Dezember 1996 siehe Spalte 4, Zeile 7 - Spalte 7, Zeile 10 ---	1
A	DE 32 25 455 A (SIEMENS AG) 19.Januar 1984 siehe das ganze Dokument ---	1
A	DE 32 34 637 A (TEVES GMBH ALFRED) 22.März 1984 in der Anmeldung erwähnt siehe das ganze Dokument ---	1
A	DE 43 41 082 A (TEVES GMBH ALFRED) 8.Juni 1995 in der Anmeldung erwähnt siehe das ganze Dokument ---	1
A	DE 41 37 124 A (TEVES GMBH ALFRED) 13.Mai 1993 in der Anmeldung erwähnt siehe das ganze Dokument ---	1
A	EP 0 346 804 A (ALSTHOM) 20.Dezember 1989 siehe das ganze Dokument ---	1
A	DE 195 29 434 A (TEVES GMBH ALFRED) 13.Februar 1997 in der Anmeldung erwähnt siehe das ganze Dokument ---	1
A	GUDEA D D ET AL: "FAULT TOLERANT POWER CONTROLLER" PROCEEDINGS OF THE INTERSOCIETY ENERGY CONVERSION ENGINEERING CONFERENCE. (IECEC), WASHINGTON, AUG. 6 - 11, 1989, Bd. VOL. 1, Nr. CONF. 24, 6.August 1989, JACKSON W D;HULL D A, Seiten 231-237, XP000078771 siehe das ganze Dokument -----	1

3

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 98/01108

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 4672530 A	09-06-1987	IN 163485 A	01-10-1988
EP 0399308 A	28-11-1990	US 5086499 A	04-02-1992
		CA 2017227 A,C	23-11-1990
		JP 3012772 A	21-01-1991
US 5583769 A	10-12-1996	JP 4133601 A	07-05-1992
		KR 9505875 B	02-06-1995
DE 3225455 A	19-01-1984	KEINE	
DE 3234637 A	22-03-1984	FR 2533183 A	23-03-1984
		GB 2127507 A,B	11-04-1984
		JP 59130768 A	27-07-1984
		US 4546437 A	08-10-1985
DE 4341082 A	08-06-1995	WO 9515518 A	08-06-1995
		EP 0731937 A	18-09-1996
		JP 9509269 T	16-09-1997
DE 4137124 A	13-05-1993	CZ 9203808 A	16-03-1994
		DE 59202984 D	24-08-1995
		WO 9309986 A	27-05-1993
		EP 0611352 A	24-08-1994
		HU 69338 A	28-09-1995
		JP 7504864 T	01-06-1995
		PL 168757 B	30-04-1996
		SK 380892 A	07-06-1995
		US 5458404 A	17-10-1995
EP 0346804 A	20-12-1989	FR 2632748 A	15-12-1989
		CN 1041465 A,B	18-04-1990
		EG 18885 A	30-11-1994
		JP 2039245 A	08-02-1990
		MX 172185 B	07-12-1993
DE 19529434 A	13-02-1997	WO 9706487 A	20-02-1997
		EP 0843853 A	27-05-1998